TRACE FORMS OF GALOIS EXTENSIONS IN THE PRESENCE OF A FOURTH ROOT OF UNITY

J. MINÁČ * AND Z. REICHSTEIN *

ABSTRACT. We study quadratic forms that can occur as trace forms $q_{L/K}$ of Galois field extensions L/K, under the assumption that K contains a primitive 4th root of unity. M. Epkenhans conjectured that $q_{L/K}$ is always a scaled Pfister form. We prove this conjecture and classify the finite groups G which admit a G-Galois extension L/K with a non-hyperbolic trace form. We also give several applications of these results.

1. INTRODUCTION

The trace form of a finite separable field extension (or, more generally of an étale algebra) L/K is the non-degenerate quadratic form $q_{L/K}\colon x \mapsto \mathrm{tr}_{L/K}(x^2)$ defined over K. In this paper we shall address the following problem: Given a finite group G, which quadratic forms over K are trace forms of G-Galois extensions L/K? This question has been extensively studied; see, e.g. [5] and the references there. In [9] D.-S. Kang and the second author obtained the following partial answer:

Theorem 1.1. *Let L/K be a G-Galois extension and let S be a Sylow 2-subgroup of G. Assume*

(a) S is not abelian, and

(b) K contains a primitive eth root of unity, where

$$e = \min\{\exp(H) \,|\, H \text{ is a non-abelian subgroup of } S\}\,.$$

Then the trace form $q_{L/K}$ is hyperbolic over K.

In this paper we will study trace forms of G-Galois extensions L/K, assuming only that K contains a primitive 4th root of unity. M. Epkenhans has conjectured that in this situation $q_{L/K}$ is always a scaled Pfister form. Our first main result is a proof of this conjecture. Before giving the precise statement, we introduce some notations.

If G is a group and $i \geq 1$ is an integer, we set $G^i = <g^i \,|\, g \in G> \lhd G$. If S is a finite 2-group, then $S^2 = \mathrm{Fr}(S)$ is the Frattini subgroup of S. The Frattini rank r of S is the rank of the elementary abelian group $S/S^2 \simeq (\mathbb{Z}/2)^r$. Note

1991 *Mathematics Subject Classification.* 11E81, 12F05, 20D15, 12J10.
Key words and phrases. Trace form, quadratic form, Witt ring, Pfister form, Galois field extension, powerful group, henselian valuation, Iwasawa structure.
*Partially supported by an NSERC research grant.

that the Frattini rank of S equals the cardinality of any minimal generating set of S; see, e.g., [18, 7.3].

Theorem 1.2. *Suppose K is a field containing a primitive 4th root of unity, L/K is G-Galois extension, S is a Sylow 2-subgroup of G, and r is the Frattini rank of S. Then the trace form $q_{L/K}$ is Witt-equivalent to the scaled Pfister form $<|S|>\otimes \ll a_1, \dots, a_r \gg$, for some $a_1, \dots, a_r \in K^*$.*

Several remarks are in order, regarding Theorem 1.2. First of all, both Theorem 1.1 and 1.2 remain true for Galois K-algebras L that are not necessarily fields. The reason is that both are enough to check for a single "versal" G-Galois algebra, which is a field; cf. e.g., [9, Proposition 2.5].

Secondly, Theorem 1.2 was previously known for $|S| \le 16$; see [5, Corollary 6, p. 227].

Thirdly, the "scaling factor" of $<|S|>$ presents only a minor inconvenience in working with the trace form $q_{L/K}$. It can be dropped if $|S|$ is a square in K (and, in particular, if K contains a primitive 8th root of unity; cf. Remark 9.1) and replaced by $<2>$ in all other cases.

Finally, the requirement that K should contain a primitive 4th root of unity is essential. Indeed, let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{2+\sqrt{2}})$. By [5, Proposition 8] (with $q = a = b = 1$ and $D = 2$), the field extension L/K is Galois, with $\mathrm{Gal}(L/K) = \mathbb{Z}/4$ and the trace form $q_{L/K} = <1, 2, 1, 1>$. This form is positive-definite and thus anisotropic. Consequently, $q_{L/K}$ cannot be Witt-equivalent to a 2-dimensional form. This shows that Theorem 1.2 fails for this extension.

Our second main result is a complete description of those finite groups G which admit a G-Galois extension L/K with a non-hyperbolic trace form. (Here we assume that K contains a primitive root of unity of degree 2^m for a fixed $m \ge 2$.) It turns out that these groups belong to a rather small but interesting family that was previously studied for entirely different reasons.

Theorem 1.3. *Let G be a finite group, S be a Sylow 2-subgroup of G and $m \ge 2$ be an integer. Then the following conditions are equivalent:*

(a) there exists a S-Galois extension E/F such that F contains a primitive root of unity of degree 2^m and the trace form $q_{E/F}$ is not hyperbolic,

(b) there exists a G-Galois extension L/K such that K contains a primitive root of unity of degree 2^m and the trace form $q_{L/K}$ is not hyperbolic,

(c) T/T^{2^m} is abelian for every subgroup T of S,

(d) there exist an integer $s \ge m$, an abelian subgroup $A \lhd S$, and an element $t \in S$ such that $S = <A, t>$ and $tat^{-1} = a^{1+2^s}$ for every $a \in A$.

A simple argument based on Sylow's theorem shows that condition (c) is equivalent to H/H^{2^m} being abelian for every subgroup H of G (see Remark 5.2). Note also that the G-Galois extension L/K in part (b) can be chosen so that $\mathrm{char}\,(K) = 0$ (see Remark 7.3) and K does not contain a primitive root of unity of degree 2^{m+1} (see Remark 5.1).

The 2-groups T appearing in condition (c) are *powerful* in the sense of Lubotzky and Mann [13]. Their results on the structure of powerful groups will be used in the proof of Theorem 1.3, along with theorems of Iwasawa [8] and Engler-Koenigsmann [6].

Theorems 1.2 and 1.3 have a natural cohomological interpretation. Let G be a finite group, S be a Sylow 2-subgroup of G, r be the Frattini rank of S and K be a field containing a primitive root of unity of degree 2^m for some integer $m \geq 2$. Then to every G-Galois field extension L/K (and, more generally, to a G-Galois K-algebra L) we can associate the well-defined cohomology class $\phi(L) = (a_1) \cdot (a_2) \dots (a_r)$ in $H^r(K, \mathbb{Z}/2\mathbb{Z})$, where $a_1, \dots, a_r$ are as in Theorem 1.2. In other words, $\phi(L)$ is the Arason invariant of the Pfister form $<|S|> \otimes q_{L/K}$; cf. [1, Section 1]. The map ϕ so defined is easily seen to be a cohomological invariant

$$\phi \colon H^1(*, G) \longrightarrow H^r(*, \mathbb{Z}/2\mathbb{Z}),$$

where $*$ ranges over the category of fields containing a primitive 2^mth root of unity. (Recall that the non-abelian cohomology set $H^1(K, G)$ parametrizes G-Galois algebras over K.) Theorem 1.3 gives equivalent conditions for this cohomological invariant to be non-trivial.

The rest of this paper is structured as follows. Theorem 1.2 is proved in Sections 2 and 3. Theorem 1.3 is proved in Sections 4 - 7. In Section 8 we discuss a number of applications of these results. In particular, we show that the trace form of a G-Galois field extension L/K is hyperbolic if the field K is "sufficiently small" in a suitable sense (see Proposition 8.1) or if G is a simple group whose Sylow 2-subgroups are non-abelian (see Proposition 8.2). In the last section we give a description of quadratic forms that can occur as trace forms of $M(2^n)$-Galois extensions, where

$$M(2^n) = < \sigma, \tau | \sigma^{2^{n-1}} = 1 = \tau^2, \tau\sigma\tau = \sigma^{1+2^{n-2}} > .$$

Acknowledgments

We would like to thank the organizers of the MSRI programs in Galois Theory and Noncommutative Algebra and MSRI staff for giving us an opportunity to meet and to begin our collaboration in the Fall of 1999. We are also grateful to M. Epkenhans, A. Pfister and J.-P. Serre for stimulating discussions, and to G. Bhandari, J.-P. Serre and the anonymous referee for helpful comments on an earlier draft of this paper.

2. Orthogonal 2-groups

Most of our subsequent results will be based on the following lemma, communicated to us by J.-P. Serre.

Lemma 2.1. *Let K be a field containing a primitive 4th root of unity, (V, q) be a non-degenerate finite-dimensional quadratic space over K and G be a finite 2-subgroup, acting orthogonally on V. Then V can be decomposed as*

an orthogonal sum $V = V^{\mathrm{Fr}(G)} \oplus V_0$, such that the restriction of q to V_0 is hyperbolic.

Here, as usual, $V^{\mathrm{Fr}(G)} = \{v \in V \mid h(v) = v \text{ for every } h \in \mathrm{Fr}(G)\}$, and we allow the trivial hyperbolic quadratic space $V_0 = \{0\}$.

Proof. We argue by induction on $\dim(V) + |G|$. Assume, to the contrary, that the lemma fails for some V, q and G; choose a counterexample with $\dim(V) + |G|$ as small as possible. Then G acts faithfully on V; otherwise we could obtain a counterexample with a smaller value of $\dim(V) + |G|$ by keeping the same V and replacing G by G/N, where N is the kernel of this action.

We claim that every index 2 subgroup of G is elementary abelian. Indeed, assume the contrary: $\mathrm{Fr}(H) \neq \{1\}$ for some index 2 subgroup H. Equivalently, $V^{\mathrm{Fr}(H)} \neq V$. Since $|H| + \dim V < |G| + \dim V$, our induction hypothesis applies and we can write V as an orthogonal sum

$$V = V^{\mathrm{Fr}(H)} \oplus V_1 \,,$$

where the restriction of q to V_1 is hyperbolic. In particular, $(V^{\mathrm{Fr}(H)}, q_{|V^{\mathrm{Fr}(H)}})$ is a regular quadratic space; see [11, p. 11, Corollary 2.6]. Since $\mathrm{Fr}(H)$ is a normal subgroup of G, the action of G restricts to $V^{\mathrm{Fr}(H)}$. This restricted action is once again orthogonal, and since $\dim V^{\mathrm{Fr}(H)} < \dim V$, we can apply our induction assumption to write $V^{\mathrm{Fr}(H)}$ as an orthogonal sum

$$V^{\mathrm{Fr}(H)} = V^{\mathrm{Fr}(G)} \oplus V_2 \,,$$

where the restriction of q to V_2 is hyperbolic. To sum up,

$$V = V^{\mathrm{Fr}(H)} \oplus V_1 = V^{\mathrm{Fr}(G)} \oplus V_0 \,,$$

where the restriction of q to $V_0 = V_1 \oplus V_2$ is hyperbolic, contradicting our choice of V and G. This contradiction proves the claim.

If every element of G has order ≤ 2 then G is itself elementary abelian. In this case the lemma is trivial, because $\mathrm{Fr}(G) = \{1\}$. Thus we may assume G has an element g of order 4. By the claim we just proved, g is not contained in any subgroup of G of index 2. In other words, $<g>$ is not contained in any proper subgroup of G, i.e., $G = <g> \simeq \mathbb{Z}/4$. We shall thus concentrate on this case for the rest of the proof. Note that $\mathrm{Fr}(G) = <g^2>$. We now proceed with an explicit description of V_0.

Now recall that K is assumed to contain a primitive 4th root of unity; we will denote it by ζ. Since $g^4 = 1$, we can decompose V as a direct sum of the four eigenspaces for g:

$$V = V_1 \oplus V_{-1} \oplus V_\zeta \oplus V_{-\zeta} \,, \tag{2.1}$$

where $V_\alpha = \{v \in V \mid g(v) = \alpha v\}$. Note that if $x \in V_\alpha$ and $y \in V_\beta$ then

$$B(x,y) = B(g(x), g(y)) = \alpha\beta B(x,y)$$

and thus

$$B(x,y) = 0 \text{ whenever } \alpha\beta \neq 1. \tag{2.2}$$

Here B denotes the bilinear form associated with the quadratic form q.

In particular $V^{\mathrm{Fr}(G)} = V_1 \oplus V_{-1}$ is orthogonal to $V_\zeta \oplus V_{-\zeta}$, and thus we can take $V_0 = V_\zeta \oplus V_{-\zeta}$. By (2.2) both V_ζ and $V_{-\zeta}$ are totally isotropic. Thus V_0 contains a totally isotropic space of dimension at least half the dimension of V_0. Observe also that from (2.2), and from our assumption that q is non-degenerate on V, it follows that q is non-degenerate on V_0. Thus we see that V_0 is hyperbolic; see [11, Chapter 1, Theorem 3.4(i)]. To sum up,

$$V = (V_1 \oplus V_{-1}) \oplus (V_\zeta \oplus V_{-\zeta}) = V^{\mathrm{Fr}(G)} \oplus V_0 \, ,$$

where the restriction of q to V_0 is hyperbolic. This contradicts our choice of G and V, thus completing the proof of Lemma 2.1. □

Corollary 2.2. *Let G be a finite 2-group and L/K be a G-Galois extension. Assume K contains a primitive 4th root of unity. Then*

(a) $q_{L/K} \simeq <|\,\mathrm{Fr}(G)|> \otimes q_{L^{\mathrm{Fr}(G)}/K}$.

(b) More generally, for any normal subgroup $H \subset \mathrm{Fr}(G)$,

$$q_{L^H/K} \simeq <[\mathrm{Fr}(G) : H]> \otimes q_{L^{\mathrm{Fr}(G)}/K} \, .$$

Here $\simeq$ denotes Witt equivalence.

Proof. (a) The 2-group G acts orthogonally on the quadratic space $(V = L, q_{L/K})$ over K. By Lemma 2.1, $q_{L/K}$ is Witt-equivalent to its restriction to $L^{\mathrm{Fr}(G)}$. Finally, for every $x \in L^{\mathrm{Fr}(G)}$, we have

$$q_{L/K}(x) = |\,\mathrm{Fr}(G)|\, q_{L^{\mathrm{Fr}(G)}}(x) \, ,$$

and part (a) follows.

(b) Apply part (a) to the G/H-Galois extension L^H/K, remembering that $\mathrm{Fr}(G/H) = \mathrm{Fr}(G)/H$. □

3. Conclusion of the proof of Theorem 1.2

As usual, given $a_1, a_2, \ldots, a_n \in K^*$, $\ll a_1, \ldots, a_n \gg = \otimes_{i=1}^n <1, -a_i>$ will denote an n-fold Pfister form. Note that since we always assume K contains a primitive 4th root of unity,

$$\ll a_1, \ldots, a_n \gg \simeq \otimes_{i=1}^n <1, a_i> .$$

We now begin the proof of Theorem 1.2 by reducing to the case where $G = S$ is a 2-group.

Lemma 3.1. *Let G be a finite group, K be a field containing a primitive 4th root of unity, L/K be a G-Galois extension, S be the Sylow 2-subgroup of G, $K_1 = L^S$ and $\phi\colon W(K) \longrightarrow W(K_1)$ be the natural (extension of scalars) homomorphism of Witt rings.*

(a) (*cf.* [2, 6.1.1]) $q_{L/K_1} = \phi(q_{L/K})$ *in* $W(K_1)$.

(b) $q_{L/K}$ *is hyperbolic if and only if* q_{L/K_1} *is hyperbolic.*

(c) Let $a \in K^*$. Then $q_{L/K} = <a> \otimes \ll a_1, \dots, a_r \gg$ in $W(K)$, for some $a_1, \dots, a_r \in K^*$, if and only if $q_{L/K_1} = <a> \otimes \ll b_1, \dots, b_r \gg$ in $W(K_1)$ for some $b_1, \dots, b_r \in K_1^*$.

Proof. (a) $\phi(q_{L/K})$ is clearly the trace form of the K_1-algebra $L_1 = L \otimes_K K_1$ and L_1 is isomorphic, as a K_1-algebra, to

$$L \oplus \cdots \oplus L \ (m \text{ times}), \tag{3.1}$$

where $m = [G : S]$ is odd. Moreover, (3.1) is an orthogonal direct sum with respect to the trace form. Thus

$$\phi(q_{L/K}) = q_{L/K_1} \oplus \cdots \oplus q_{L/K_1} \ (m \text{ times});$$

cf. [3, Theorem I.5.1]. Since we are assuming K (and thus K_1) contains a primitive 4th root of unity, $2W(K_1) = \{0\}$, and part (a) follows.

By Springer's theorem, ϕ is injective; see, e.g., [11, Theorem 7.2.3]. Part (b) now follows from (a).

(c) By Rost's theorem on the descent of Pfister forms [16, Section 3] (see also [2, 4.4.1]), $<a> \otimes q_{L/K}$ is Witt-equivalent to a Pfister form over K if and only if $<a> \otimes q_{L/K_1}$ is Witt-equivalent to a Pfister form over K_1. □

We now continue with the proof of Theorem 1.2. By Lemma 3.1(c) we may assume that G is a 2-group. By Corollary 2.2

$$q_{L/K} \simeq <|\operatorname{Fr}(G)|> \otimes q_{L^{\operatorname{Fr}(G)}/K}.$$

Note that $L^{\operatorname{Fr}(G)}/K$ is a $G/\operatorname{Fr}(G)$-Galois extension, where $G/\operatorname{Fr}(G) \simeq (\mathbb{Z}/2)^r$. Thus it is enough to prove Theorem 1.2 in the case where $\operatorname{Gal}(L/K)$ is an elementary abelian 2-group; indeed, if we know that

$$q_{L^{\operatorname{Fr}(G)}/K} \simeq <|G/\operatorname{Fr}(G)|> \otimes (r\text{-fold Pfister form}).$$

then by Corollary 2.2(a)

$$q_{L/K} \simeq <|\operatorname{Fr}(G)|> \otimes q_{L^{\operatorname{Fr}(G)}/K} \simeq <|G|> \otimes (r\text{-fold Pfister form}),$$

as claimed.

Now assume $G = (\mathbb{Z}/2)^r$. Here any G-Galois extension L/K has the form $L = K(\sqrt{a_1}, \dots, \sqrt{a_r})$, for some $a_1, \dots, a_r \in K^*$, and an easy computation in the basis $\{a_1^{\frac{\epsilon_1}{2}} \dots a_r^{\frac{\epsilon_r}{2}}\}$, with $\epsilon_1, \dots, \epsilon_r = 0, 1$, shows that

$$q_{L/K} \simeq <2^r> \otimes \ll a_1, \dots, a_r \gg; \tag{3.2}$$

cf. [2, 6.2.1] or [9, Lemmas 2.1(b) and 2.2]. This completes the proof of Theorem 1.2. □

4. Iwasawa structures

An *Iwasawa structure of level* $s \geq 1$ on a 2-group G is a normal abelian subgroup A and an element t such that $G = <A, t>$ and

$$tat^{-1} = a^{1+2^s} \text{ for every } a \in A.$$

Informally speaking, the higher the level is, the closer G is to an abelian group. In particular, if $\exp(A) = 2^e$ and $s \geq e$ then G is abelian. Conversely, any finite abelian 2-group G of exponent $\leq 2^s$ admits an Iwasawa structure of level s, with $A = G$ and $t = \{1\}$.

If a 2-group G admits an Iwasawa structure of level ≥ 2, we will call G an Iwasawa group. Note that the level of an Iwasawa group G is not well-defined in general, since G may admit Iwasawa structures of different levels (see Example 4.2 below).

For any 2-group G we define the *strength* of G by

$$\operatorname{str}(G) = \max \{m \mid G/G^{2^m} \text{ is abelian}\}.$$

In particular, $\operatorname{str}(G) = \infty$ iff G is abelian and $\operatorname{str}(G) \geq 2$ iff G is *powerful* in the sense of Lubotzky and Mann; cf. [13, Definition, p. 499].

Lemma 4.1. *Suppose that G is a finite 2-group which admits an Iwasawa structure (A, t) of level s. Then*

(a) $[G, G] = A^{2^s}$*,*

(b) $\operatorname{str}(G) \geq s$*,*

(c) If $s \geq 2$ *then* $G^{2^m} = <A^{2^m}, t^{2^m}>$ *for every* $m \in \mathbb{N}$*.*

Proof. (a) From the definition of an Iwasawa structure of level s, we see that $A^{2^s} \subset [G, G]$ and G/A^{2^s} is abelian. Hence, $[G, G] = A^{2^s}$.

(b) By part (a) G/A^{2^s} is commutative. Hence, so is G/G^{2^s}, and part (b) follows.

(c) By part (b), $\operatorname{str}(G) \geq 2$. Thus $[G, G] \subset G^4$, i.e., G is a powerful 2-group. The desired conclusion now follows from [4, Theorem 2.7]. □

We remark that part (c) remains true even if $s = 1$. This stronger assertion will not be used in the sequel; we leave it as an exercise for the reader.

Example 4.2. The inequality $\operatorname{str}(G) \geq s$ may be strict, even if G is non-abelian. Indeed, let

$$G = <a, t | a^{2^5} = 1, a^{2^2} = t^{2^3}, tat^{-1} = a^{1+8}>.$$

One checks readily that G is a metacyclic group of order 2^8 and that G admits an Iwasawa structure (A, t) of level 3, where $A = <a>$. We claim that $\operatorname{str}(G) = 4$. By Lemma 4.1, $[G, G] = <a^8>$. Since $a^8 = t^{16}$, we see that $[G, G]$ is contained in G^{16} but not in $G^{32} = <a^{32}, t^{32}> = <a^{16}>$. Thus $\operatorname{str}(G) = 4$, as claimed.

On the other hand, observe that G admits another Iwasawa structure $(\widetilde{A}, \widetilde{t})$ of level 4, where $\widetilde{A} = <t>$ and $\widetilde{t} = a^{-1}$. Indeed, have $\widetilde{t}\,t\,\widetilde{t}^{-1} = a^{-1}ta = t^{1+2^4}$. Thus we see that by switching the role of t and a^{-1}, we are able to find another Iwasawa structure whose level equals the strength of G. In the next lemma we shall show that such a switch is always possible.

Lemma 4.3. *Suppose G be a non-abelian Iwasawa 2-group. Then*

$$\mathrm{str}(G) = \max\{\mathit{level}(A,t)\}\,,$$

where the maximum is taken over all Iwasawa structures (A,t) on G.

Proof. Let $m = \mathrm{str}(G)$ and (A,t) is an Iwasawa structure on G of level s. By Lemma 4.1, $s \leq m$. If $s = m$ we are done. Thus we may assume $s < m$. Our goal is to construct another Iwasawa structure on G of level m.

Since G is an Iwasawa 2-group, $m \geq 2$. Thus $[G,G] \subset G^4$, so that G is a powerful group. By Lemma 4.1,

$$A^{2^s} = [G,G] \subset G^{2^m} = <A^{2^m}, t^{2^m}>\,.$$

We now see that the group G^{2^m}/A^{2^m} is cyclic, and hence, so is its subgroup A^{2^s}/A^{2^m}. Since $s < m$ this implies that A^{2^s} is itself cyclic.

Let $a^{2^s} = t^{2^m}$ be a generator of A^{2^s} with $a \in A$. Since the order of a is equal to the exponent of A, we see that there exists a subgroup B of A such that $A = <a> \oplus B$. Moreover, since A^{2^s}/A^{2^m} is cyclic, we see that $B^{2^s} = \{1\}$. Therefore, $tbt^{-1} = b^{1+2^s} = b$ for each $b \in B$, and B is a subgroup of the center $Z(G)$ of G.

Set $\widetilde{A} = <t, B>$ and $\widetilde{t} = a^{-1}$. We claim that $(\widetilde{A}, \widetilde{t})$ is an Iwasawa structure on G of level m. First we have

$$<\widetilde{A}, \widetilde{t}> = <t, B, a^{-1}> = <t, A> = G.$$

Also $\widetilde{A}$ is an abelian subgroup of G as $B \subset Z(G)$. Further $\widetilde{t}\,t\,\widetilde{t}^{-1} = a^{-1}ta = a^{-1}a^{1+2^s}t = a^{2^s}t = t^{1+2^m}$, as $a^{2^s} = t^{2^m}$. Because $\widetilde{A} = <B, t>$ and $B \subset Z(G)$ we see that $\widetilde{t}\,\widetilde{a}\,\widetilde{t}^{-1} = \widetilde{a}^{\,1+2^m}$ for each $\widetilde{a} \in \widetilde{A}$. Hence $(\widetilde{A}, \widetilde{t})$ is the Iwasawa structure of level m. □

Remark 4.4. In view of Lemma 4.3, a 2-group S satisfies condition (d) of Theorem 1.3 if and only if it is an Iwasawa group of strength $\geq m$.

5. Proof of Theorem 1.3 (a) $\Longrightarrow$ (b) $\Longrightarrow$ (c) $\Longrightarrow$ (d)

(a) $\Longrightarrow$ (b): Let k be the subfield of F generated by the prime field and the primitive 2^mth root of unity and let V be a faithful linear representation of G over k (e.g., we can take V to be the group algebra $k[G]$). Denote the field of rational functions on V by $k(V)$. Since the trace form of the S-Galois extension E/F is not hyperbolic [9, Proposition 2.5] tells us that the trace form of $k(V)/k(V)^S$ is not hyperbolic. Now by Lemma 3.1(b), $k(V)/k(V)^G$ is not hyperbolic either. Thus we can take $L = k(V)$ and $K = k(V)^G$.

(b) $\Longrightarrow$ (c): Let L/K be a G-Galois field extension with a non-hyperbolic trace form, as in (b). Assume, to the contrary, that T/T^{2^m} is non-abelian for some subgroup T of S. Then the trace form of L/L^T is still non-hyperbolic; see [9, Lemma 2.1(c)]. Thus, replacing G by T and K by L^T, we may assume $G = T$.

Now let $H = G^{2^m}$. Then L^H/K is a Galois extension with Galois group G/H, which by our assumption, is non-abelian of exponent $\leq 2^m$. Thus, by Theorem 1.1, $q_{L^H/K}$ is hyperbolic. Now, since $H \subset G^2 = \mathrm{Fr}(G)$, Corollary 2.2 tells us that $q_{L/K}$ is hyperbolic as well, contradicting our assumption.

(c) $\Longrightarrow$ (d): By our assumption every subgroup T of S satisfies $[T, T] \subset T^4$, i.e., T is powerful. By [13, Theorem 4.3.1] this implies that S is modular but not Hamiltonian. On the other hand, by a theorem of Iwasawa [8] modular non-Hamiltonian 2-groups are precisely the 2-groups that admit an Iwasawa structure of of level ≥ 2. [1]

It remains to show that S admits an Iwasawa structure of level $s \geq m$. First suppose S is abelian. Then, as we pointed out in Section 4, we can take $A = S$, $t = 1$, and $s = \max\{m, e\}$, where e is the exponent of S. Now assume S is not abelian. Then by our assumption (c), $\mathrm{str}(S) \geq m$. The desired conclusion now follows from Lemma 4.3. $\square$

Remark 5.1. *If* char $(K) = 0$ *then the G-Galois extension L/K in part (b) can be chosen so that K does not contain a primitive root of unity of degree 2^{m+1}.*

Proof. Let $k = \mathbb{Q}(\zeta_{2^m})$ be the subfield of K generated by its prime subfield and a primitive 2^mth root of unity. Let $V = k^n$ be a faithful G-representation (over k), as in the proof of the implication $(a) \Longrightarrow (b)$. Since the trace form of the S-Galois extension E/F is not hyperbolic, [9, Proposition 2.5] tells us that the trace form of $k(V)/k(V)^S$ is not hyperbolic. Thus we can replace E by $E' = k(V)$ and F by $F' = k(V)^G$. Since k is algebraically closed in E', E' (and hence, F') does not contain a primitive root of unity of degree 2^{m+1}. $\square$

The same argument goes through in characteristic p, provided that $k = \mathbb{F}_p(\zeta_{2^m})$ does not contain $\zeta_{2^{m+1}}$.

Remark 5.2. *Condition (c) of Theorem 1.3 is equivalent to*

(c$'$) H/H^{2^m} is abelian for every subgroup H of G.

Proof. Clearly, (c$'$) $\Longrightarrow$ (c). To prove the converse, let T be a Sylow 2-subgroup of H. After replacing S by a conjugate Sylow subgroup in G, we may assume $T \subset S$. Let $\overline{T}$ be the image of T in H/H^{2^m}. We claim that $\overline{T} = H/H^{2^m}$. Indeed, on the one hand, the exponent of H/H^{2^m} divides 2^m, so that H/H^{2^m} is a 2-group. On the other hand, since T is a Sylow

[1] The proofs of Iwasawa's theorem in [8] and [20, Theorem 14] had some gaps that were later pointed out and closed by Napolitani [14]. For a detailed exposition of Iwasawa's theorem and related group-theoretic results, we refer the reader to [17].

2-subgroup of H, the index $[H : T]$ is odd. The index of $\overline{T}$ in H/H^{2^m} is thus both odd and a power of 2; hence, $\overline{T} = H/H^{2^m}$, as claimed.

Consequently,

$$T/T^{2^m} \overset{\text{onto}}{\longrightarrow} T/(T \cap H^{2^m}) \simeq H/H^{2^m}\,.$$

If T/T^{2^m} is abelian, then so is H/H^{2^m}. This shows that (c) $\Longrightarrow$ (c′). □

Remark 5.3. Let G be a finite group. If A and B are subgroups of G, we shall denote the set of intermediate subgroups $A \subset X \subset B$ by $[A, B]$. This set is naturally a lattice, where $X \wedge Y = X \cap Y$ and $X \vee Y =$ subgroup generated by X and Y.

Let S be a Sylow 2-subgroup of G. Suppose for some subgroups A and B of S, the map $\varphi_{A,B} : [A,\, A \vee B] \longrightarrow [A \wedge B,\, B]$, defined by $\varphi_{A,B}(X) = A \wedge X$, is not a lattice isomorphism. Then the trace form $q_{L/K}$ is hyperbolic for every G-Galois extension L/K such that K contains a primitive 4th root of unity.

Proof. If $\varphi_{A,B}$ is not a lattice isomorphism for some A and B then the lattice $[\{1\}, S]$ is not modular; see [17, Theorem 2.1.5]. Then, by Iwasawa's theorem (the easy direction), S does not satisfy condition (d) of Theorem 1.3. The desired conclusion follows from the implication (b) $\Longrightarrow$ (d). □

6. Proof of Theorem 1.3 (d) $\Longrightarrow$ (a): Preliminary reductions

We begin by observing that for the purpose of proving the implication $(d) \Longrightarrow (a)$, we may assume that $G = S$ is a 2-group and that $m = s$. We shall say that S admits a non-hyperbolic trace form if it satisfies condition (a) of Theorem 1.3.

It is easy to see that every abelian 2-group admits a non-hyperbolic trace form; see, e.g., [9, Remark 3.2]. Thus we will assume from now on that S is non-abelian. Recall that by our assumption (d), $S = <A, t>$, where A is abelian and

$$tat^{-1} = a^{1+2^s} \text{ for every } a \in A. \tag{6.1}$$

Our proof of the implication (d) $\Longrightarrow$ (a) of Theorem 1.3 will consist of two parts. In this section we will reduce the problem to the case where $A = (\mathbb{Z}/2^e\mathbb{Z})^r$ and S is a semidirect product of A and $<t>$; in the next section we will show that every S of this form admits a non-hyperbolic trace form. (Note that here r is the Frattini rank of A; the Frattini rank of S is $r + 1$.)

In order to facilitate working with Iwasawa groups, we will write them in terms of generators and relations. Decompose the abelian 2-group

$$A = <a_1> \times \cdots \times <a_r> \simeq \mathbb{Z}/2^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/2^{e_r}\mathbb{Z}\,,$$

as a product of cyclic subgroups, where a_i has order 2^{e_i}. Then $\exp(A) = 2^e$, where $e = \max\{e_1, \dots, e_r\}$. Since S is non-abelian,

$$s < e\,. \tag{6.2}$$

Denote the order of the image of t in G/A by 2^q and let $a_0 = t^{2^q} \in A$. Note that the order of a_0 in A is $2^{-q}|{<}t{>}|$ and, since a_0 commutes with t, $a_0^{2^s} = 1$ in A.

Lemma 6.1. *(a) The group* $X = A * {<}t{>}/{<}tat^{-1} = a^{1+2^s} \,|\, a \in A{>}$ *is isomorphic to* $A \rtimes {<}t{>}$*, with the action of* t *on* A *given by* (6.1)*. Here* $A * {<}t{>}$ *denotes the free product of the subgroups* A *and* ${<}t{>}$ *of* G*.*

(b) Let $c \in A$ *be an element of order* $2^{-q}|{<}t{>}|$*, satisfying* $c^{2^s} = 1$ *and* $Y = A * {<}t{>}/{<}t^{2^q} = c\,,\ tat^{-1} = a^{1+2^s} \,|\, a \in A{>}$*. Then every element of* Y *can be uniquely written in the form* at^i *for some* $a \in A$ *and* $0 \le i < 2^q$*.*

(c) S *is isomorphic to* $Z = A * {<}t{>}/{<}t^{2^q} = a_0\,,\ tat^{-1} = a^{1+2^s} \,|\, a \in A{>}$*.*

Proof. (a) Consider the natural surjective homomorphism $X \longrightarrow A \rtimes {<}t{>}$, taking a to a and t to t. Since X has at most $|A| \times |{<}t{>}|$ elements (every element of X can be written in the form at^i for some $a \in A$ and $0 \le i < |{<}t{>}|$), this homomorphism is an isomorphism.

(b) The defining relations of Y tell us that every element of Y can be written as at^i, with $a \in A$ and $i \in \{0, 1, \dots, 2^q - 1\}$. To prove uniqueness, it is enough to show that $|Y| = 2^q \cdot |A|$. Note that Y is the quotient of $X = A \rtimes {<}t{>}$ by the central cyclic subgroup $C = {<}ct^{-2^q}{>}$. (This subgroup is central in X because $c^{2^s} = 1$ in A.) Since c has order $2^{-q}|{<}t{>}|$ in A and t^{2^q} has order $2^{-q}|{<}t{>}|$ in ${<}t{>}$, we have $|C| = 2^{-q}|{<}t{>}|$

$$|Y| = \frac{|X|}{|C|} = \frac{|A| \cdot |{<}t{>}|}{|C|} = 2^q |A|\,,$$

as desired.

(c) Every element of S can be uniquely written in the form at^i, for some $a \in A$ and $0 \le i < 2^q$. Thus the natural surjective homomorphism $Z \longrightarrow S \simeq {<}A, t{>}$ is an isomorphism. □

We are now ready to prove the main result of this section. We will continue to use the notations of Lemma 6.1.

Reduction 6.2. In the proof of the implication $(d) \Longrightarrow (a)$ of Theorem 1.3 we may assume without loss of generality that

(1) $e_1 = \cdots = e_r$ and

(2) S is a semidirect product of A and ${<}t{>}$.

Proof. We will use the following two simple "moves" to go from an arbitrary Iwasawa group to one satisfying (1) and (2):

(i) If H is a subgroup of G and G admits a non-hyperbolic trace form then so does H.

(ii) Suppose T is a 2-group and N be a normal subgroup of T contained in $T^2 = \mathrm{Fr}(T)$. If T admits a non-hyperbolic trace form then so does T/N.

(ii) is immediate from Corollary 2.2. To prove (i), note that if the trace form of a G-Galois extension L/K is not hyperbolic then neither is the trace form of L/L^H; see, e.g., [9, Lemma 2.1(c)]

(1) Let $e = \max\{e_1, \dots, e_r\}$ and embed A in the abelian group

$$B = <b_1> \times \cdots \times <b_r> \simeq \mathbb{Z}/2^e \times \cdots \times \mathbb{Z}/2^e \, ,$$

where each b_i has order 2^e and $a_i = b_i^{2^{e-e_i}}$ for all $i = 1, 2, \dots, r$. Let

$$S_1 = B * <t>/<t^{2^q} = a_0 \, , \; tbt^{-1} = b^{1+2^s} \, | \, b \in B> .$$

Then there is a natural homomorphism $S \simeq Z \longrightarrow S_1$, which sends t to t and a to a for every $a \in A \subset B$. By Lemma 6.1(b), this homomorphism is injective. Thus by (i) we may replace S by S_1. This completes the proof of (1).

From now on, we will assume that $e_1 = \cdots = e_r = e$.

(2) Let X and Z be as in Lemma 6.1. Consider the natural homomorphism $f \colon X \longrightarrow Z \simeq S$ which sends t to t and a to a for every $a \in A$. By Lemma 6.1(a) $X \simeq A \rtimes <t>$. It now suffices to show that $\mathrm{Ker}(f) \subset \mathrm{Fr}(X) = X^2$; part (2) will then follow from (ii), with $T = X$. For notational convenience, we will denote the image t in S by $\overline{t}$.

Suppose $at^i \in \mathrm{Ker}(f)$ for some $a \in A$ and $0 \le i < |<t>|$; in other words, $a\overline{t}^{\,i} = 1$ in S. Then, since the order of $\overline{t}\,A$ in S/A is 2^q, we conclude that i is a multiple of 2^q. In particular, since S is not abelian, we have $q \geq 1$ and thus $t^i \in X^2$. It remains to show that $a \in X^2$. Indeed, since $a = \overline{t}^{\,-i}$ in S, a and $\overline{t}$ commute in S, i.e., $a^{2^s} = 1$ in S. Since we are assuming that $A \simeq (\mathbb{Z}/2^e\mathbb{Z})^r$ and $s < e$, cf. part (1) and (6.2), we conclude that $a \in A^2$ in A, and consequently $a \in X^2$ in X, as claimed. $\square$

7. Conclusion of the proof of Theorem 1.3 (d) $\Longrightarrow$ (a)

In view of Reduction 6.2, it remains to prove the following

Proposition 7.1. *Let $S = A \rtimes <t>$, where $<t>$ is a finite cyclic 2-group, acting on $A = (\mathbb{Z}/2^e\mathbb{Z})^r$ by $tat^{-1} = a^{1+2^s}$, and $2 \le s < e$. Then there exists a S-Galois extension E/F such that F contains a primitive root of unity ζ_{2^s} of degree 2^s and the trace form $q_{E/F}$ is non-hyperbolic.*

Our proof of Proposition 7.1 below relies on valuation theory; our primary background references are [6], [15] and [22]. We shall denote the finite field of order q by $\mathbb{F}_q$.

Lemma 7.2. *For every integer $s \geq 2$, there exists a field F with a 2-henselian valuation v with value group Γ_v, and residue field $\mathcal{K}$, such that*

(i) $\mathrm{char}\, \mathcal{K} \neq 2$,

(ii) F contains a primitive root of unity ζ_{2^s} of degree 2^s but does not contain the primitive root of unity $\zeta_{2^{s+1}}$ of degree 2^{s+1},

(iii) $\dim_{\mathbb{F}_2} \Gamma_v/2\Gamma_v \geq r$.

(iv) $\mathcal{K}(2) = \mathcal{K}(\zeta_{2^\infty})$, where $\mathcal{K}(\zeta_{2^\infty})$ is the extension of $\mathcal{K}$ obtained by adjoining all 2^nth roots of unity to $\mathcal{K}$, for $n = 1, 2, \dots$ and $\mathcal{K}(2)$ is the maximal 2-extension of $\mathcal{K}$ in some algebraic closure of $\mathcal{K}$.

Moreover, we can choose F so that $\mathrm{char}\,(F) = 0$.

Proof. We shall give two constructions: a simple one in prime characteristic and a slightly more complicated one in characteristic zero.

Construction 1: Observe that $5^{2^{s-2}} - 1$ is divisible by 2^s but not by 2^{s+1} for any integer $s \geq 2$; see, e.g., [18, 5.3.17]. Therefore if $q = 5^{2^{s-2}}$ then $\zeta_{2^s} \in \mathbb{F}_q$ but $\zeta_{2^{s+1}} \notin \mathbb{F}_q$. Let $F = \mathbb{F}_q((X_1))((X_2))\ldots((X_r))$ be the field of the iterated power series in variables $X_1, \ldots, X_r$ over $\mathbb{F}_q$ and v be the natural 2-henselian valuation $v : F \longrightarrow \mathbb{Z} \times \cdots \times \mathbb{Z}$ (r-times), where $\mathbb{Z} \times \cdots \times \mathbb{Z}$ is lexicographically ordered. One also has $\mathcal{K}(v) = \mathbb{F}_q$, so that properties (i)-(iv) hold.

Construction 2: Alternatively consider the field

$$F = \mathbb{Q}_p((x_1))((x_2))\ldots((x_r))$$

of characteristic 0 and the natural 2-henselian valuation

$$v\colon F \longrightarrow \mathbb{Z} \times \cdots \times \mathbb{Z} \; (r \text{ times}).$$

This valuation composed with the p-adic valuation on $\mathbb{Q}_p$ (see e.g., [15, p. 63]) yields a new 2-henselian valuation $v' : F \longrightarrow \mathbb{Z} \times \cdots \times \mathbb{Z}$ ($(r+1)$-times) with a residue field $\mathcal{K}(v') = \mathbb{F}_p$. (The fact that v' is again 2-henselian follows from [15, Proposition 10, page 211]; see also [10, p. 4].) Thus v' satisfies conditions (i), (iii) and (iv).

It remains to show that we can choose the prime p so that condition (ii) holds. We claim that for each $s \in \mathbb{N}$ there is a prime p such that $\zeta_{2^s} \in \mathbb{Q}_p$ but $\zeta_{2^{s+1}} \notin \mathbb{Q}_p$. By Hensel's Lemma it is enough to show that for each $s \in \mathbb{N}$ there exists a prime p such that $p-1$ is divisible by 2^s but not by 2^{s+1}. To construct p, note that by Dirichlet's theorem there exists $n \in \mathbb{N}$ such that $p = (1+2^s) + 2^{s+1}n$ is a prime number; this prime p has the desired properties. □

For the rest of this section, we shall assume that F, v, Γ_v and $\mathcal{K}$ are as in Lemma 7.2, $\mathbb{Z}_2$ is the additive group of 2-adic integers and furthermore,

- $F(2)$ is the maximal 2-extension of F in some algebraic closure,
- $G_F(2) := \mathrm{Gal}(F(2)/F)$ is the Galois group of $F(2)/F$,
- $T_v \simeq \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$ (d-times), where $d = \dim_{F_2} \Gamma_v/2\Gamma_v$. Here T_v denotes the inertia subgroup of $G_F(2)$ associated with v,
- w is the unique valuation of $F(2)$ which extends v on F.

By a result of Engler and Koenigsmann [6, Proposition 1.1b],

$$G_F(2) \simeq (T_v \times G_{\mathcal{K}(\zeta_{2^\infty})}(2)) \rtimes \mathbb{Z}_2\,,$$

where $\mathbb{Z}_2 =< \sigma >$ and the action of σ on T_v is $\sigma^{-1}\tau\sigma = \tau^{2^s+1}$ for every $\tau \in T_v$.

It is also worthwhile to recall that T_v/T_v^2 is the Pontrjagin dual of $\Gamma_v/2\Gamma_v$, and this duality is induced by the Kummer pairing

$$< \; , \; > : T_v/T_v^2 \times \Gamma_v/2\Gamma_v \longrightarrow \{\pm 1\}\,,$$

where $<[\theta]\,,\,[f]> \,=\, \theta(\sqrt{f})/\sqrt{f}$ for each $\theta \in T_v$ and $f \in F^*$. Here $[\theta] \in T_v/T_v^2$ and $[f] \in \Gamma_v/2\Gamma_v$ denote the images in θ and f in the factor groups T_v/T_v^2 and $\Gamma_v/2\Gamma_v$, respectively.

We are now ready to finish the proof of Proposition 7.1. Suppose $G_{\mathcal{K}(\zeta_{2^\infty})}(2) = \{1\}$, i.e., $\mathcal{K}(2) = \mathcal{K}(\zeta_{2^\infty})$. Then we have

$$G_F(2) \simeq T_v \rtimes \mathbb{Z}_2.$$

Since $d = \dim_{\mathbb{F}_2} \Gamma_v/2\Gamma_v \geq r$ we deduce that

$$T_v = \underbrace{\mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2}_{r \text{ times}} \times S$$

for some suitable subgroup S of T_v. Therefore there exists a surjective homomorphism $\widetilde{\varphi} : T_v \longrightarrow A$ which projects the first factor on A and is trivial on S. Because the action of σ on T_v is given by $\sigma^{-1}\tau\sigma = \tau^{1+2^s}$ for each $\tau \in T_v$, we see that $\widetilde{\varphi}$ extends uniquely to a surjective homomorphism

$$\varphi : G_F(2) \longrightarrow S \text{ such that } \varphi(\sigma) = t^{-1}.$$

Let R be the kernel of φ and E the fixed field of R. Then E/F is Galois and $\mathrm{Gal}(E/F) \simeq S$. From the fact that $T_v \simeq \mathrm{Hom}(\Gamma_w/\Gamma_v, \zeta_{2^\infty})$ (see [6, page 2474]) and the fact that the outer factor $\mathbb{Z}_2$ in the semidirect decomposition of $G_F(2)$ as $T_v \rtimes \mathbb{Z}_2$ is $\mathrm{Gal}(F(\zeta_{2^\infty})/F)$, we see that the maximal Galois subextension E'/F of E/F with a Galois group of exponent 2 has the form

$$E' = F(\sqrt{a_1}, \ldots, \sqrt{a_r}, \zeta_{2^{s+1}}),$$

where $a_1, a_2, \ldots, a_r \in F^*$ such that their values $v(a_1), \ldots, v(a_r) \in \Gamma_v$ are linearly independent in $\Gamma_v/2\Gamma_v$ over $\mathbb{F}_2$.

From [22, Proposition 4.7] we see that the Pfister form

$$\ll a_1, \ldots, a_r, \zeta_{2^s} \gg$$

is non-hyperbolic. By Corollary 2.2 the trace form of E/F is Witt equivalent to a scalar multiple of $\ll a_1, \ldots, a_r, \zeta_{2^s} \gg$, which is also non-hyperbolic. This completes the proof of Proposition 7.1 and thus of Theorem 1.3. □

Remark 7.3. Our proof shows that if the equivalent conditions (a) - (d) of Theorem 1.3 hold then the fields F and K in parts (a) and (b) can be chosen to be of characteristic zero.

8. Applications

Trace forms over "small" fields.

Proposition 8.1. *Let G be a finite group, S be a Sylow 2-subgroup of G, K be a field containing a primitive 4th root of unity and L/K be a G-Galois extension. Denote the Frattini rank of S by r.*

(a) If K is a C_{r-1}-field then the trace form $q_{L/K}$ is hyperbolic.

(b) If $\mathrm{cd}_2(K) \leq r - 1$ then the trace form $q_{L/K}$ is hyperbolic.

(c) If K is a number field and $r \geq 3$ (i.e., S cannot be generated by two elements) then the trace form $q_{L/K}$ is hyperbolic.

Here $\mathrm{cd}_2(K)$ refers to the 2-cohomological dimension of K. For the definition of cohomological dimension and of the C_i property for fields, see [19, II.4].

Proof. By Theorem 1.2 it is enough to show that under the assumptions of the corollary every r-fold Pfister form q over K is hyperbolic.

In part (a) q is necessarily isotropic and, hence, hyperbolic; see, e.g., [11, Corollary 10.1.6]. In part (b), by Milnor's conjecture (recently proved by Voevodsky [21]) q lies in I^{r+1}, where I is the fundamental ideal in the Witt ring $W(K)$ and by the Arason-Pfister theorem this is only possible if q is hyperbolic; see [11, Corollary 10.3.4].

Part (c) is a special case of (b), since a totally imaginary number field has cohomological dimension 2; see [19, II.4.4]. However, a much more elementary argument, based on the Hasse-Minkowski principle, is available in this case. Indeed, every quadratic form of dimension ≥ 5 over K is isotropic; see [11, Corollary 3.5, p. 169]. In particular, for $r \geq 3$, every r-fold Pfister form is isotropic and hence hyperbolic over K. □

Simple groups.

Proposition 8.2. *Let G be a finite simple group and let S be the Sylow 2-subgroup of G. Then the following are equivalent.*

(a) S is abelian, and

(b) There exists a G-Galois field extension L/K such that K contains a primitive 4th root of unity and the trace form $q_{L/K}$ is not hyperbolic.

Proof. By Theorem 1.3 it is sufficient to prove that S cannot be a non-abelian Iwasawa group. Equivalently (via Iwasawa's theorem [8]) S cannot be a non-abelian modular non-Hamiltonian 2-group. The last assertion is an immediate consequence of [24, Proposition 4.2]. (It can also be deduced from [17, page 197, Exercise 1].) □

For the sake of completeness we remark if a finite simple group G has an abelian 2-Sylow subgroup S then S is necessarily elementary abelian (see [7, Theorem 4.2.3]); moreover, Walter [23] classified all finite simple groups G with this property.

The extension problem. Let G be a finite group and N be a normal subgroup of G and $K \subset L$ be a G/N-Galois field extension. Recall that the *extension problem* for this data is the question of existence of a tower $K \subset L \subset M$, such that M/K is a G-Galois field extension, and the natural quotient map $\mathrm{Gal}(M/K) \longrightarrow \mathrm{Gal}(L/K)$ coincides with $G \longrightarrow G/N$.

Now assume that G is a nonabelian 2-group of Frattini rank r, $N = \mathrm{Fr}(G) = G^2$, and $L = K(\sqrt{a_1}, \dots, \sqrt{a_r})$ is a multiquadratic extension of K of degree 2^r such that $\mathrm{Gal}(L/K) \cong G/\mathrm{Fr}(G) = (\mathbb{Z}/2\mathbb{Z})^r$. Assume also that K contains a primitive eth root of unity, where

$$e = \min\{\exp(H) \mid H \text{ is a non-abelian subgroup of } G\}.$$

Proposition 8.3. *If the extension problem for G, N, and L/K defined above has a solution, then the r-fold Pfister form $\ll a_1, \ldots, a_r \gg$ is a hyperbolic over K.*

Proof. Suppose L/K is the required G-Galois field extension. Then from Theorem 1.1 we see that the trace form $q_{L/K}$ is hyperbolic. But from Corollary 2.2(a) we see that $q_{L/K}$ is Witt equivalent to a scalar multiple of $\ll a_1, \ldots, a_r \gg$. Hence $\ll a_1, \ldots, a_r \gg$ is hyperbolic as required. □

9. Which quadratic forms are trace forms?

We now return to the question we posed at the beginning of the Introduction. Let G be a finite group and K be a field containing $\sqrt{-1}$. Which quadratic forms q over K can occur as trace forms of G-Galois field extension L/K? In view of Theorem 1.3 we may assume that the Sylow 2-subgroup S of G is an Iwasawa 2-group; otherwise every trace form will be hyperbolic. By Theorem 1.2

$$q \simeq |S| \otimes (r\text{-fold Pfister form})$$

but, in general, we do not know which r-fold Pfister forms can occur, even if $G = S$ is a 2-group. In this section we will describe the trace forms for one particular family of groups.

Recall that the modular group $M(2^n)$ of order 2^n is defined as

$$M(2^n) = <\sigma, \tau \,|\, \sigma^{2^{n-1}} = 1 = \tau^2, \tau\sigma\tau = \sigma^{1+2^{n-2}}> .$$

In the sequel

(9.1) we will always assume that $n \geq 4$.

It is easy to see that $M(2^n)$ is an Iwasawa group of order 2^n, exponent 2^{n-1} and strength $n-2$. Setting $A = <\sigma>$, we see that (A, τ) is an Iwasawa structure on $M(2^n)$ of level $n-2$. Note also that the Frattini subgroup of $M(2^n)$ is $\mathrm{Fr}(M(2^n)) = <\sigma^2>$.

For future reference we record the following elementary observation. As usual, we shall denote the class of $a \in K^*$ in $K^*/(K^*)^2$ by $[a]$.

Remark 9.1. Let K be a field containing a primitive 4th root of unity ζ_4. Then $2\zeta_4 = (1+\zeta_4)^2$ and thus

(9.2) $$[2] = [\zeta_4] \text{ in } K^*/(K^*)^2.$$

In particular,

(i) if K contains a primitive 8th root of unity then 2 is a square in K and

(ii) if K contains a primitive root of unity $\zeta_{2^{n-2}}$ then 2^n is a square in K.

Indeed, (i) is immediate from (9.2). To prove (ii), consider two cases: $n = 4$ and $n \geq 5$; see (9.1). If $n = 4$ then $2^4 = 4^2$ is certainly a square. For $n \geq 5$ (cf. (9.1)), (ii) follows from (i).

We now proceed with the main result of this section. As usual, ζ_i will denote a primitive ith root of unity.

Proposition 9.2. *Let $n \geq 4$ be an integer, K be a field such that $\zeta_{2^{n-2}} \in K$ but $\zeta_{2^{n-1}} \notin K$ and q be a non-degenerate 2^n-dimensional quadratic form over K. Then the following are equivalent:*

(a) q is Witt equivalent to the trace form of some $M(2^n)$-Galois field extension L/K.

(b) q is Witt equivalent to $\ll \zeta_{2^{n-2}}, a \gg$ for some $a \in K^*$, where $[a] \neq [1]$, $[\zeta_{2^{n-2}}]$ in $K^*/(K^*)^2$.

Our assumption that $\zeta_{2^{n-1}} \notin K$ is harmless, since otherwise Theorem 1.1 tells us that the trace form of every $M(2^n)$-Galois extension is hyperbolic. On the other hand, the assumption that $\zeta_{2^{n-2}} \in K$ is essential.

Proof. Set $K' = K(\zeta_{2^{n-1}})$, where $\zeta_{2^{n-1}}$ is a primitive root of unity of degree 2^{n-1}. By our assumption on K, $[K' : K] = 2$.

(b) $\Longrightarrow$ (a): Suppose $q \simeq \ll \zeta_{2^{n-2}}, a \gg$, where $a \neq [1]$, $[\zeta_{2^{n-2}}]$ in $K^*/(K^*)^2$. We will construct an $M(2^n)$-Galois extension L/K whose trace form is Witt equivalent to q by modifying [9, Example 6.1], due to Serre.

Let $L = K'(\sqrt[2^{n-1}]{a})$. By our assumption on $[a]$, a is not a square in K'. Thus $[L : K'] = 2^{n-1}$ (see, e.g., [12, Theorem VIII.9.16]) and consequently, $[L : K] = 2^n$. Now the computations in [9, Example 6.1] show that L/K is an $M(2^n)$-Galois extension whose trace form $q_{L/K}$ is Witt equivalent to $<2^n> \otimes \ll \zeta_{2^{n-2}}, a \gg$. Finally by Remark 9.1(ii), 2^n is a square in K and thus the factor of $<2^n>$ can be removed. In other words, q is Witt equivalent to $\ll \zeta_{2^{n-2}}, a \gg$, as claimed.

(a) $\Longrightarrow$ (b): Assume that $q = q_{L/K}$ for some $M(2^n)$-Galois extension L/K. Then $q \otimes_K K'$ is the trace form of the $M(2^n)$-Galois K'-algebra $L \otimes_K K'$. By Theorem 1.1, we know that $q \otimes_K K'$ is hyperbolic. (Recall that Theorem 1.1 applies to Galois algebras as well as field extensions; see the first remark after the statement of Theorem 1.2 in Section 1.) On the other hand, combining Theorem 1.2 and Remark 9.1, we see that q is Witt equivalent to a 2-fold Pfister form. The basic theory of Pfister forms (see, e.g., [1, p. 465]) now tells us that q is Witt equivalent to $\ll \zeta_{2^{n-2}}, a \gg$ for some $a \in K^*$.

It remains to show that a can always be chosen so that $[a] \neq [1]$, $[\zeta_{2^{n-2}}]$ in $K^*/(K^*)^2$. Note that if $[a] = [1]$ or $[\zeta_{2^{n-2}}]$ then $\ll \zeta_{2^{n-2}}, a \gg$ is a hyperbolic trace form. Thus in order to finish the proof of the proposition, it suffices to establish assertions (i) and (ii) below. Recall that a field K containing a primitive 4th root of unity ζ_4 is called *rigid* if and only if for every $k \notin (K^*)^2$, the form $<1, k>$ represents only the classes $[1]$ and $[k]$ in $K^*/(K^*)^2$; cf. [25, Section 3].

(i) If K is rigid then no $M(2^n)$-Galois field extension L/K has a hyperbolic trace form.

(ii) If K is not rigid then $\ll \zeta_{2^{n-2}}, b \gg$ is hyperbolic for some $b \in K^*$ such that $[b] \neq [1]$, $[\zeta_{2^{n-2}}]$ in $K^*/(K^*)^2$.

In other words, if K is rigid then the case where $[a] = [1]$ or $[\zeta_{2^{n-2}}]$ can never occur. If K is not rigid then, after possibly replacing a by b, we can always assume that $[a] \neq [1]$, $[\zeta_{2^{n-2}}]$ in $K^*/(K^*)^2$.

To prove (i), note that if L/K is an $M(2^n)$-Galois extension then $L^{\mathrm{Fr}(M(2^n))}$ is a $\mathbb{Z}/2 \times \mathbb{Z}/2$-Galois extension of K. Hence, $L^{\mathrm{Fr}(M(2^n))}$ has the form $K(\sqrt{a}, \sqrt{b})$ for some $a, b \in K^*$, where a and b are $\mathbb{F}_2$-linearly independent in $K^*/(K^*)^2$. By Corollary 2.2(a),

$$q \simeq <|\,\mathrm{Fr}(M(2^n))|> \otimes\, q_{K(\sqrt{a},\sqrt{b})/K}\,.$$

Here $|\,\mathrm{Fr}(M(2^n))| = 2^{n-2}$ because $\mathrm{Fr}(M(2^n))$ is the cyclic subgroup of $M(2^n)$ generated by σ^2. Combining this with formula (3.2) for $q_{K(\sqrt{a},\sqrt{b})/K}$, we obtain

$$q \simeq <2^n>\otimes \ll a, b \gg \simeq \ll a, b \gg\,,$$

where the factor of $<2^n>$ can be removed in view of Remark 9.1(ii). Over a rigid field such a form cannot be isotropic, since otherwise $<1, a>$ would take on the same value as $<b> \otimes <1, a>$, thus making $[a]$ and $[b]$ linearly dependent over $\mathbb{F}_2$. This proves (i).

To prove (ii), we appeal to [25, Theorem 2.16(2)], which tells us that over a non-rigid field K the form $<1, \zeta_{2^{n-2}}>$ assumes a value b such that $[b] \neq [1]$, $[\zeta_{2^{n-2}}]$ in $K^*/(K^*)^2$. Then $\ll \zeta_{2^{n-2}}, b \gg$ is hyperbolic, as claimed. $\square$

Remark 9.3. Suppose $n = 4$. Then by Remark 9.1, we can replace the form $\ll \zeta_4, a \gg$ in the statement of Proposition 9.2 by $\ll 2, a \gg$. This way we recover [5, Corollary 6(b)] for $G = M(16)$.

References

1. J. K. Arason, *Cohomologische Invarianten Quadratischer Formen*, J. of Algebra **36** (1975), 448–491.
2. E. Bayer-Fluckiger and J.-P. Serre, *Torsions quadratiques et bases normales autoduales*, Amer. J. Math. **116** (1994), no. 1, 1–64.
3. P. E. Conner, R. Perlis, *A survey of trace forms of algebraic number fields*, Series in Pure Mathematics, **2**, World Scientific Publishing Co., Singapore, 1984.
4. J. D. Dixon, M. P. F. du Sautoy, A. Mann, and D. Segal, *Analytic pro-p groups*, second ed., Cambridge University Press, Cambridge, 1999.
5. C. Drees, M. Epkenhans, and M. Krüskemper, *On the computation of the trace form of some Galois extensions*, J. Algebra **192** (1997), no. 1, 209–234.
6. A. J. Engler and J. Koenigsmann, *Abelian subgroups of pro-p Galois groups*, Trans. Amer. Math. Soc. **350** (1998), no. 6, 2473–2485.
7. W. Feit, *The current situation in the theory of finite simple groups*, ACTES, Congrès Intern. Math., Tome 1 (1970), 55–93.
8. K. Iwasawa, *Über die endlichen Gruppen und die Verbände ihrer Untergruppen*, J. Fac. Sci. Imp. Univ. Tokyo. Sect. I. **4** (1941), 171–199.
9. D.-S. Kang and Z. Reichstein, *Trace forms of Galois field extensions in the presence of roots of unity*, J. Reine Angew. Math. **549** (2002), 79–89.
10. J. Koenigsmann, *Solvable absolute Galois groups are metabelian*, Invent. Math. **144** (2001), 1–22.

11. T. Y. Lam, *The algebraic theory of quadratic forms*, Benjamin/Cummings Publishing Co. Inc. Advanced Book Program, Reading, Mass., 1980, Revised second printing, Mathematics Lecture Note Series.
12. S. Lang, *Algebra*, Addison-Wesley Publishing Co., Inc., 1965.
13. A. Lubotzky and A. Mann, *Powerful p-groups. I. Finite groups*, J. Algebra **105** (1987), no. 2, 484–505.
14. F. Napolitani, *Sui p-gruppi modulari finiti*, Rend. Sem. Mat. Univ. Padova, **39** (1967), 296–303.
15. P. Ribenboim, *Théorie des Valuations*, Les Presses de L'Université de Montréal, 1965.
16. M. Rost, *A descent property for Pfister forms*, J. Ramanujan Math. Soc. **14** (1999), no. 1, 55–63.
17. R. Schmidt, *Subgroup lattices of groups*, De Gruyter Expositions in Mathematics **14**, Walter De Gruyter, Berlin, 1994.
18. W. R. Scott, *Group theory*, second ed., Dover Publications Inc., New York, 1987.
19. J.-P. Serre, *Galois cohomology*, Springer-Verlag, Berlin, 1997.
20. M. Suzuki, *Structure of a group and the structure of its lattice of subgroups*, Springer-Verlag, Berlin, 1956.
21. V. Voevodsky, *Voevodsky's Seattle lectures: K-theory and motivic cohomology*, Algebraic K-theory (Seattle, WA, 1997), Amer. Math. Soc., Providence, RI, 1999, pp. 283–303.
22. A. R. Wadsworth, *p-Henselian field: K-theory, Galois cohomology, and graded Witt rings*, Pacific J. Math. **105** (1983), no. 2, 473–496.
23. J. H. Walter, *The characterization of finite groups with abelian Sylow-2-subgroups*, Ann. Math. **89** (1969), 405–514.
24. H. N. Ward, *Automorphisms of quaternion-free 2-groups*, Math. Z. **112** (1969), 52–58.
25. R. Ware, *Valuation rings and rigid elements in fields*, Canad. J. Math. **33** (1981), no. 6, 1338–1355.

Department of Mathematics, University of Western Ontario, London, Ontario N6A 5B7, Canada

E-mail address: `minac@uwo.ca`

Department of Mathematics, University of British Columbia, Vancouver, BC, Canada V6T 1Z2

E-mail address: `reichst@math.ubc.ca`